Table of Contents

Table of Contents 1
Приложения 2
- Требования к сетевому окружению 3
- Установка сертификата локального удостоверяющего центра 6
- Опции DHCP 12
- Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0 15
- Синтаксис языка запросов 19

Приложения

Требования к сетевому окружению

Product: SWG
Version: 7.5.x

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8001	Входящий (до веб-консоли UserGate SWG)	Доступ к веб-интерфейсу управления устройством.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4040	Входящий (к UserGate по API)	Управление устройством UserGate по API.
XML-RPC поверх HTTPS	TCP	4443	Входящий (к UserGate по API)	Доступ к API поверх HTTPS
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверам технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)/Входящий (от клиентов до сервера UserGate, если он используется в качестве сервера точного времени)	Синхронизация времени.
DNS	TCP/UDP	53	Входящий (от клиентов к серверу UserGate, если он выступает в качестве DNS-сервера)	Сервис получения информации (IP-адрес) о доменах.
	UDP	53	Исходящий (до серверов DNS)	
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Регистрация продуктов UserGate: доступ до сервера reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)
Связь с UserGate Management Center	TCP	9712	Исходящий (от UG SWG до UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Management Center.
		2022	Исходящий (от UG SWG до UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
		9713	Входящий (от LogAn к UG SWG)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Log Analyzer.

Связь с UserGate Log Analyzer	Сервис	TCP Протокол	Порт	Исходящий/Входящий	Функция
			2023	Входящий (от LogAn к UG SWG)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Подключение конечных устройств с установленным ПО UserGate Client		TCP	4045	Входящий (от конечного устройства на UG SWG)	Подключение конечных устройств и приём телеметрии для проверки комплаенса.
LDAP		TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL).
Captive-портал и страница блокировки		TCP	443, 8043	Входящий (от браузера клиента на UG SWG)	Отображение страницы авторизации Captive-портала и страницы блокировки.
Kerberos		TCP/UDP	88	Исходящий (на сервер аутентификации Kerberos)	Аутентификация пользователей по протоколу Kerberos.
NTLM		TCP	445	Исходящий (на сервер аутентификации NTLM)	Аутентификация пользователей по протоколу NTLM.
RADIUS		UDP	1812	Исходящий (на сервер аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS.
TACACS+		TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
Агент терминального сервиса		UDP	1812, 1813	Входящий (от агента на UG SWG)	Доступ к серверу UserGate, необходимый для работы терминального агента.
Агент аутентификации для Windows		UDP	1812, 1813	Входящий (от агента на UG SWG)	Доступ к серверу UserGate, необходимый для работы агента аутентификации доменных пользователей, работающих на ОС Windows.
Прокси-агент		UDP	8090	Входящий (от агента на UG SWG)	Доступ к серверу UserGate, необходимый для работы прокси-агента, предоставляющего доступ в Интернет пользователям, работающим на ОС Windows.
SNMP		UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.
SMTP		TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
ICAP		TCP	1344	Исходящий (до серверов ICAP)	Сервис работы с серверами ICAP.
DHCP		UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)/Входящий (UserGate выступает в качестве DHCP-сервера)	Сервис службы DHCP.
BGP		TCP	179	Исходящий (передача информации соседним BGP-маршрутизаторам)/Входящий (получение информации от соседних BGP-маршрутизаторов)	Сервис динамической маршрутизации BGP.
OSPF		89/OSPF		Исходящий (передача информации соседним OSPF-маршрутизаторам /Входящий (получение информации от соседних OSPF-маршрутизаторов)	Сервис динамической маршрутизации OSPF.

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
RIP	UDP	520	Исходящий (распространение соседним маршрутизаторам RIP-маршрутов)/Входящий (получение от соседних маршрутизаторов RIP-маршрутов)	Сервис динамической маршрутизации RIP.
FTP (экспорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экспорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экспорт журналов)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.

Установка сертификата локального удостоверяющего центра

Product: SWG
Version: 7.5.x

Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика.

Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

Откройте папку, куда вы скачали pem-сертификат, переименуйте его в user.der и дважды нажмите на него:

Откроется информация о сертификате. Нажмите **Установить сертификат**:

Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:

Выберите хранилище сертификата и нажмите **Обзор**:

Выберите **Доверенные корневые центры сертификации** и нажмите **ОК**:

Нажмите **Готово**:

Когда появится предупреждение системы безопасности, нажмите **Да**:

Установка сертификата завершена.

Установка сертификата в браузер Safari, Chrome в macOSX

Перейдите в папку, куда вы скачали pem-сертификат и дважды нажмите на него:

Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:

Введите свой пароль для подтверждения данной операции:

Сертификат установлен.

Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется одинаково для всех операционных систем. Рассмотрим установку на примере ОС Windows.

Откройте настройки браузера Firefox (**Инструменты → Настройки**):

Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите **Просмотр сертификатов**:

Нажмите **Импортировать** и укажите путь к скачанному PEM-сертификату:

Установите флажок **Доверять при идентификации веб-сайтов** и нажмите **ОК**:

Установка сертификата завершена.

Опции DHCP

Product: SWG
Version: 7.5.x

Формат значений опций соответствует RFC 2132.

Наименование	Описание
1	Маска подсети, из которой был получен адрес.
2	Разница во времени в подсети клиента относительно UTC (указывается в секундах).
3	Список IP-адресов доступных шлюзов.
6	Список DNS-серверов.
7	Список лог-серверов (MIT-LCS UDP).
9	Список LPR-серверов (RFC 1179).
13	Размер загрузочного образа для клиентов.
15	Имя домена.
16	Swap-сервер.
17	Путь корневого каталога для клиента.
18	Путь расширений BOOTP.
19	Применение пересылки IP-датаграмм.
20	Использование маршрутизации удаленного источника.
21	Политика фильтрации IP-адресов.
22	Максимальный размер датаграммы.
23	Значение TTL для IP по умолчанию.
26	Значение MTU для данного интерфейса.
27	Признак, что все подсети используют текущую конфигурацию MTU.
31	Определение использования сообщений ICMP для обнаружения маршрутизаторов.
32	Адрес, который используется для обращения к маршрутизатору.
33	Статичный список маршрутизации; состоит из пар «адрес назначения» — «адрес роутера».
34	Использование концевиков (trailers) при запросах ARP.
35	Тайм-аут кэш-памяти ARP.

Наименование	Описание
36	Необходимость использования инкапсуляции данных Ethernet.
37	Значение TTL для TCP-пакетов.
38	Интервал отправки контрольных пакетов TCP (TCP keep-alive).
40	Домен NIS.
41	Список серверов NIS.
42	Список серверов времени NTP.
44	Список IP-адресов серверов NetBIOS.
45	Список IP-адресов серверов рассылки датаграмм NetBIOS.
46	Тип узла NetBIOS.
47	Область NetBIOS.
48	IP-адреса серверов шрифтов X Windows (X Window System Font).
49	Диспетчер дисплея X Windows.
58	Время T1 — интервал времени, в течение которого клиент должен отправить запрос на обновление IP-адреса.
59	Время T2 — интервал времени (в секундах), в течение которого клиент должен отправить запрос на повторное связывание.
60	Опция используется клиентом DHCP для указания поставщика.
64	Имя домена NIS+.
65	Список серверов NIS+.
66	Имя сервера TFTP.
67	Название загрузочного файла.
68	Адреса домашних агентов (Mobile IP Home Agent).
69	Список серверов SMTP.
70	Список серверов POP3.
71	Список серверов NNTP.
74	Список серверов IRC.
77	Класс пользователя.

Наименование	Описание
80	Опция позволяет получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
93	Архитектура системы клиента DHCP.
94	Идентификатор сетевого интерфейса клиента DHCP.
97	Идентификатор клиента на основе UUID/GUID.
119	Список поиска DNS.
120	Список серверов SIP.
121	Список бесклассовых статических маршрутов.
125	Указание информации о поставщике.
255	Конец списка опций; обязательно должен присутствовать последним.

Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0

Product: SWG
Version: 7.5.x

Категории Министерства Образования РФ	**Категории UserGate URL filtering 4.0**
Peer-To-Peer	Пиринговые сети
Алкоголь. Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию	Алкоголь и табак
Баннеры и рекламные программы Баннерные сети, всплывающая реклама, рекламные программы	Реклама и всплывающие окна
Библиотеки	Искусство
Вождение и автомобили	Транспорт
Вредоносное программное обеспечение	Нелегальное ПО
Вредоносные программы	Ботнеты
	Сайты сомнительного содержания
	Вредоносное ПО
	Криптомайнеры
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечение	Поздравительные открытки
	Развлечения
	Мода и красота
	Отдых и оздоровление
	Рестораны и еда
	Спорт
	Путешествия

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Здоровье и медицина	Здоровье и медицина
	Половое воспитание
Злоупотребление свободой СМИ - информация с ограниченным доступом. Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций	Оружие
Злоупотребление свободой СМИ - информация, содержащая скрытые вставки и иные технические способы воздействия на под-104№ п/п Тематическая категория Содержание скрытое воздействие сознание людей и (или) оказывающая вредное влияние на их здоровье	Сайты сомнительного содержания
Злоупотребление свободой СМИ - наркотические средства, сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Ненависть и нетерпимость
	Насилие
Злоупотребление свободой СМИ -экстремизм Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы	Ненависть и нетерпимость
	Насилие
Знакомства	Знакомства
Информация с ограниченным доступом. Информация, составляющая государственную или иную охраняемую законом тайну	Политика
	Правительство
Информация, пропагандирующая порнографию	Порнография и насилие
Компьютерные игры	Игры
Корпоративные сайты	Бизнес
	Финансы
	Общие
	Недвижимость
Корпоративные сайты, интернет-представительства негосударственных учреждений	Некоммерческие и неправительственные организации
Личная и немодерируемая информация. Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники,	Персональные сайты
	Частные IP-адреса
	Социальные сети

блоги **Категории Министерства Образования РФ**	**Категории UserGate URL filtering 4.0**
	Потоковое мультимедиа и загрузки
	Веб-почта
Модерируемые доски объявлений (ресурсы данной категории, содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты	Социальные сети
	Чаты
Наркотические средства. Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Наркотики
Нелегальная помощь школьникам и студентам. Банки готовых рефератов, эссе, дипломных работ и пр.	Школьные мошенничества
Ненадлежащая реклама. Информация, содержащая рекламу алкогольной продукции и табачных изделий	Алкоголь и табак
Неприличный и грубый юмор. Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека	Сайты сомнительного содержания
Нижнее белье, купальники	Нудизм
Обеспечение анонимности пользователя, обход контентных фильтров. Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам	Анонимайзеры
	Переводчики
Образовательные ресурсы	Образование
Онлайн-казино и тотализаторы	Азартные игры
Отправка SMS с использованием интернет-ресурсов. Сайты, предлагающие услуги по отправке SMS-сообщений	Реклама и всплывающие окна
Платные сайты	Паркованные домены
Поиск работы, резюме, вакансии	Поиск работы
Преступления - Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию)	Преступная деятельность
Преступления-клевета, экстремизм	Преступная деятельность
Программное обеспечение	Компьютеры и технологии
	Нелегальное ПО
	Информационная безопасность

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения. Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение	Ненависть и нетерпимость
Религии и атеизм	Религиозные культы
	Религия
Система поиска изображений	Обмен картинками
	Поисковые системы и порталы
СМИ	Форумы и новостные ленты
	Новости
Табак, реклама табака, пропаганда потребления табака. Сайты, пропагандирующие потребление табака; реклама табака и изделий из него	Алкоголь и табак
Торговля и реклама	Реклама и всплывающие окна
	Покупки
Убийства, насилие	Жестокое обращение с детьми
	Насилие
Чаты	Чаты
	Сервисы мгновенных сообщений
Экстремистские материалы или экстремистская деятельность (экстремизм)	Ненависть и нетерпимость

Синтаксис языка запросов

Product: SWG
Version: 7.5.x

Язык запросов используется в веб-консоли для расширенного поиска и фильтрации данных в разделах правил и журналов.

При составлении запросов используются доступные параметры, значения этих параметров, а также логические операторы и операторы сравнения.

Запрос состоит из одного или нескольких условий, каждое из которых имеет вид:

<параметр запроса> <оператор> <значение параметра запроса>

Набор доступных параметров для запросов зависит от раздела веб-консоли. Параметры определяются свойствами правил или полями сообщений соответствующих журналов.

ПримечаниеПри вводе запросов вы можете заключать значения параметров в кавычки. Если значение параметра содержит пробелы, использование кавычек обязательно (например, 'значение 1' или "значение 2"). Для группировки нескольких условий в запросе допускается использовать круглые скобки.

Вы можете просматривать список всех параметров запросов, доступных в выбранном разделе веб-консоли устройства, используя в строке запроса символ «,» (запятая).

Для каждого параметра вы можете просматривать список доступных операторов. Для этого после ввода параметра в строке запроса необходимо нажать клавишу «Пробел».

Полный список операторов, которые могут встречаться в запросах с различными параметрами, приведен в таблице.

Оператор	Значение	Пример запроса	Примечания
Логические операторы			
AND	И (выполняются все условия)	ipSource = 198.51.100.13 AND action = deny	—
OR	Или (выполняется одно из условий)	severity = info OR severity = warning	—

Оператор	Значение	Пример запроса	Примечания
Операторы сравнения			
=	Равно (полностью совпадает)	ipSource = 192.0.2.53	—
!=	Не равно (не совпадает)	ipSource != 192.0.2.55	—
<	Меньше	statusCode < 404	Оператор применим к параметрам, поддерживающим сравнение значений (например, date, portSource, portDest или statusCode)
>	Больше	statusCode > 200	
<=	Меньше либо равно	date <= 2019-03-28T20:59:59	
>=	Больше либо равно	date >= 2019-03-13T21:00:00	
IN	Равно одному из перечисленных в скобках значений	category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')	В качестве значений параметров ipSource и ipDest можно указывать адреса подсетей в формате CIDR
NOT IN	Не равно перечисленным в скобках значениям	ipDest NOT IN (203.0.113.0/24)	
~	Содержит подстроку	ipSource ~ 203.0.113	Оператор применим к параметрам, имеющим строковые значения, без учета регистра
!~	Не содержит подстроку	browser !~ Mozilla/5.0	
MATCH	Совпадает с регулярным выражением	details MATCH NAT	Оператор использует синтаксис регулярных выражений библиотеки RE2. Описание библиотеки см. на сайте github.com в разделе компании Google
NOT MATCH	Не совпадает с регулярным выражением	details NOT MATCH NAT	

Также вы можете просматривать возможные значения некоторых параметров запросов. Для этого в строке запроса необходимо ввести параметр и оператор, а затем нажать клавишу «Пробел».